B. Remarks

Claims 1-20 are pending in the application. The examiner has rejected claims 1, 5, 11, and 15 under 35 U.S.C. § 102(b) as being anticipated by Ganesan, U.S. Patent No. 5,557,678. The examiner has rejected claims 2-4, 6-8, 12-14, and 16-18 under 35 U.S.C. § 103(a) as being unpatentable over Ganesan in view of Patel, U.S. Publication No. 2002/0071558 A1. Applicants respectfully traverse the foregoing bases for rejection.

Applicants' present invention is directed to a method for securely providing encryption keys for encrypting and decrypting data. According to the present invention, an initial software product for use on a hardware product is encrypted using an encryption key. The encryption key is split into two components by generating a first key portion and calculating the second key portion using the first key portion and the key, such that the combination of the first key portion and the second key portion yield the key. The first and second key portions and the encrypted initial software product are provided to a user. The first and second key portions are combined to yield the key, which is used to decrypt the initial software product. As such, the same key is used both to encrypt and decrypt the data. These limitations are articulated in claim 1 (and, therefore, in each of its dependent claims 2-10), which recites:

> A method for enabling encryption and decryption of an initial version of a software product comprising the steps of:
>
> generating a first encryption key;
>
> encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product;
>
> generating a first key portion of said first encryption key;

calculating a second key portion by utilizing said first key portion and said first encryption key to generate a said second key portion such that the combination of said first key portion and second key portion form said first encryption key;

providing said first key portion and said second key portion and said encrypted initial software product for use in a hardware product;

combining said first key portion and said second key portion to provide said first encryption key in said hardware product; and

utilizing said first encryption key to decrypt said encrypted initial software product in said hardware product.

The examiner has stated that Ganesan discloses the foregoing limitations, namely, generating a first encryption key, encrypting a message (which the examiner has equated with an initial software product) with the first encryption key to generate an encrypted message, generating a first key portion of said first encryption key, calculating a second key portion of said first encryption key, providing said first key portion and said second key portion and said encrypted message, combining said first key portion and said second key portion to provide said first key portion, and decrypting the message using the first and second portion of the key, the first and second key portions being the first encryption key.

Applicants respectfully traverse the examiner's assessment of Ganesan and submit that Ganesan does not teach the foregoing combination of limitations. Applicants agree that Ganesan teaches splitting certain encryption keys, namely first and second users' respective private keys, into two portions. Importantly, however, Ganesan does not teach or suggest using these private keys to encrypt or decrypt a message or an initial software product. Rather, Ganesan teaches using a different encryption key, namely, a session key, for encrypting and decrypting a message. Ganesan does not teach or suggest splitting the session key into two components.

Although Ganesan teaches the use of encryption techniques to securely distribute the session key to the first and second users, Ganesan does not teach or suggest using a user's private

encryption key to encrypt the session key, splitting the user's private encryption key into first and second portions, providing the encrypted session key and first and second key portions to the user, combining the first and second key portions to yield the user's private key, and using the user's private key to decrypt the session key. Instead, Ganesan teaches encrypting a first copy of the session key for use by the first user using the first user's public key and the first portion of the first user's private key, providing this encrypted session key to the first user, and decrypting this encrypted session key using the second portion of the first user's private key. Ganesan further teaches encrypting and decrypting a second copy of the session key for use by the second user in a similar manner using the second user's public key and first and second portions of the second user's private key.

Based on at least the above arguments, Applicants respectfully submit that claim 1 and claims 2-10 that depend from claim 1 distinguish over and are allowable over the cited references. Claim 11 and, therefore, each of dependent claims 12-20 that depend from claim 11 recite limitations similar to those set forth in claim 1. Accordingly, Applicants submit that these claims also distinguish over and are allowable over the cited references. Applicants submit that the examiner's rejections of dependent claims 2-4, 6-8, 12-14, and 16-18 under 35 U.S.C. § 103(a) are moot in view of the above. As such, Applicants respectfully submit that the pending claims are allowable over the cited references and respectfully request reconsideration toward that end.

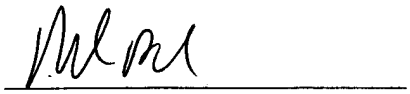
Applicants hereby amend the specification to include the government interest statement required by 35 U.S.C. § 202(c)(6).

Applicants note that the examiner has not initialed the Information Disclosure Statement submitted by Applicants on July 19, 2002 in connection with European Publication No. EP 0 478

969 A1. Applicants respectfully request that the examiner consider this reference and initial the Information Disclosure Statement accordingly.

Respectfully submitted,

Date: April 14, 2005



Mark P. Vrla
Registration No. 43,973
Attorney for Applicant

JENNER & BLOCK LLP
One IBM Plaza
Chicago, IL 60611
Ph. (312) 222-9350
Fax (312) 840-7657